As a Senior Security Engineer, you will provide expert analysis and robustly engineered solutions to help identify and combat threats to game security and integrity. The role requires an insightful, agile, and pragmatic approach to a fast changing landscape - balancing both long term capability buildout and also being able to react to newly emerging threats. This is a hands-on role, requiring strong programming and reverse-engineering skills. Working as part of an overall engineering team effort, you would be expected to both lead individual projects through to completion, in addition to playing a role in a longer term technology and capability build-out.

KEY RESPONSIBILITIES

- Create machine learning models to help investigations into game cheating, driven by technical and heuristic indicators and other criteria.
- Integrate analysis models into data pipeline, allowing continuous and batch processing of telemetry data.
- Perform R&D into both new techniques and technologies.
- Drive hypotheses, perform trial analysis, provide insights and recommendations to the security team.
- Reverse engineering to identify malware, code hijacking, and other malicious behavior.
- Provide security analysis to the internal security team.
- Identify emerging threats, propose countermeasures, implement countermeasures in a timely manner.
- Be a proactive part of the team to monitor and measure effectiveness in anti-cheat efforts.
- Support both engineering and security operations efforts.

QUALIFICATIONS
Required

- Working knowledge of Machine Learning techniques and best practices.
- Extensive knowledge of Intel-family processor architecture, mobile processors (such as ARM64) a plus.
- C/C++ development, including some understanding of assembly code.
- Reverse engineering, advanced debugging, ability to identify code vulnerabilities and exploits.
- Must have worked in a security-oriented role on previously published games.
- Be able to interact with and work directly with game engineering teams.